

## **Rationale for RBAC Protection Profile**

### **B.1 Introduction**

This rationale material is evaluation evidence and as an aid to evaluation, it is divided into sections that parallel the APE assurance class.

### **B.2 RBAC Security objectives**

The CC requires that the PP security objectives are properly categorized as applied to the TOE or its security environment, are useful and meaningful objectives, and can be shown to cover all of the threats and organizational security policies identified.

The rationale aims to demonstrate that the objectives identified provide a complete coverage of the threats and policies.

#### **B.2.1 Satisfaction of organizational security policies**

This section demonstrates that a TOE (in its environment) which meets all of the stated security objectives will effectively meet all of the identified organizational security policies.

**P.ACCESS** Access rights to specific data objects are determined by the owner of the object, the role of the subject attempting access, and the implicit and explicit access rights to the object granted to the role by the object owner.

**O.ADMIN** asserts that the TOE management possesses the necessary management tools to ensure that the TOE enforces the security policy.

**O.DUTY** provides for separation of duties, an important objective of role-based access control.

**O.HIERARCHICAL** provides for defining roles as part of other roles, which facilitates the definition of implicit and explicit access rights.

**O.ROLE** ensures that no user may perform any operation on an object without being assigned to a

role permitting that operation.

O.INSTALL (Environment) asserts that the management support will control users adequately.

### **B.2.2 Threats to be addressed by the TOE**

This section demonstrates that a TOE (in its environment) which meets all of the stated security objectives will effectively counter all of the identified threats.

**T.ACCESS** A user may gain access to resources or perform operations for which no access rights have been granted.

O.ACCOUNT mitigates this threat by providing accountability for attempts at unauthorized access.

O.ADMIN asserts that the TOE management possesses the necessary management tools to ensure that the TOE enforces the security policy.

O.AUDIT mitigates this threat by keeping records of attempts at unauthorized access.

O.KNOWN asserts that legitimate users will be identified, so access to objects can be constrained to such users.

O.ROLE counters T.ACCESS directly.

O.INSTALL (Environment) asserts that the management support will control users adequately.

**T.ENTRY** An unauthorized person may gain logical access to the TOE.

O.ADMIN ensures that the management capabilities exist to permit observation and control of potential intrusion attempts.

O.AUDIT supports the administrator in detecting attempted access by unauthorized persons.

O.ENTRY counters T.ENTRY explicitly.

O.CONNECTION (Environment) asserts that intrusion emanating from uncontrolled network sources is controlled.

O.INSTALL (Environment) asserts that the management support can and does control intrusion.

O.PHYSICAL (Environment) asserts that potential intruders cannot gain access through direct assault on the TOE.

### **B.2.3 Threats to be addressed by the operating environment**

This section demonstrates that the threats to be countered by the security environment of the TOE map to the security objectives identified for the environment.

**T.OPERATE** Security failures may occur because of improper administration and operation of the TOE.

O.CONNECT (Environment) asserts that the TOE management controls external connections so that the TOE security is not undermined.

O.INSTALL (Environment) directly asserts that TOE management accepts the responsibility for countering this threat.

**T.ROLEDEV** The development and assignment of user roles may be done in a manner that undermines security.

O.INSTALL (Environment) directly asserts that the TOE management will develop and assign roles in a manner that maintains security.

### **B.2.4 Completeness of objectives**

Table B.1 below shows the mapping of each objective, both IT and non-IT, to the environmental assumptions, threats, and policies.

**Table B.1 - Mapping objectives to threats and organizational security policies**

<b>Security Objective</b>	<b>Environmental Assumptions</b>	<b>Threats</b>	<b>Organizational Security Policies</b>
O.ACCOUNT		T.ACCESS	
O.ADMIN		T.ACCESS T.ENTRY	P.ACCESS
O.AUDIT		T.ACCESS T.ENTRY	
O.DUTY		T.ACCESS	P.ACCESS
O.ENTRY		T.ENTRY	
O.HIERARCHICAL		T.ACCESS	P.ACCESS
O.KNOWN		T.ACCESS	
O.ROLE		T.ACCESS	P.ACCESS
O.CONNECT (E)	A.CONNECT	T.ENTRY T.OPERATE	
O.INSTALL (E)	A.ACCESS A.MANAGE A.OWNER	T.ACCESS T.ENTRY T.OPERATE T.ROLEDEV	P.ACCESS
O.PHYSICAL (E)	A.ASSET A.LOCATE A.PROTECT	T.ENTRY T.PHYSICAL	

Table B.1 indicates that all objectives contribute to the ability of the TOE to counter a threat and/or satisfy a policy and that all threats and policies have been addressed. Thus, there are no unnecessary objectives.

No evaluation evidence is offered specifically in support of the claim that the objectives are sufficient to satisfy fully all threats and organizational security policies. Evaluators should consider the merits of the discussion of each threat and policy.

### **B.3 RBAC PP Functional Requirements Rationale**

This section provides the justification for the inclusion of each of the components from the relevant security functional requirements (SFR) classes, as well as the reason for the exclusion of certain other components, in the RBAC PP. The arguments establishing the relevancy of these SFR classes themselves for the RBAC PP are given in the following 3 paragraphs.

RBAC is mainly an access control mechanism. Hence, unlike the PPs for Class of products like Firewalls or Operating Systems, the RBAC PP security functional requirements cannot be a complete system security requirement. The TSF in the context of a RBAC PP must provide functions

that will enable the management of access control through the abstraction mechanism of roles. The TSF should therefore have functions that will enable the following:

- (i) Creation & Deletion of roles
- (ii) Creation, Deletion and Modification of Role Attributes
- (iii) Creation, Deletion and Modification of Role Relationships
- (iv) Creation, Deletion and Modification of Constraints on Role Relationships
- (v) Assignment & De-assignment of Users to Roles
- (vi) Specification & Maintenance of Constraints for assigning Users to Roles
- (vii) Assignment & De-assignment of Privileges to Roles
- (viii) Specification & Maintenance of Constraints for assigning Privileges to Roles

The security functional requirements that have been specified are therefore geared towards secure operation of the above functions as well maintaining the integrity of data that is needed by and created by the above functions. These requirements are covered by the following classes and form the core set of requirements for a RBAC PP.

- (a) FMT - Security Management
- (b) FDP - User Data Protection
- (c) FPT - Protection of Trusted Functions

In addition a certain minimal set of supporting requirements are needed to provide the proper environment for realizing the objectives of the core RBAC functions. These include:

- (d) Supporting the concept of proper identification and authentication and assignment of security attributes to users
- (e) Creation and Maintenance of Audit logs - to record events pertaining to the operation of core RBAC functions as well as those relating to the access to objects for which access control is enforced through these functions.
- (f) Selection of user security attributes defined for a RBAC context in a TOE session and authorization and denial of session creation based on the values of these attributes.

The families under the classes FIA (Identification and Authentication), FAU (Security Audit) and FTA (TOE Access) meet the objectives (d), (e) and (f) respectively.

### **B.3.1 Rationale for Security Audit (FAU) Class Components**

The objectives behind the choice of audit functional requirements for RBAC PP are the following:

- (a) To ensure that the relationship specified among the roles and the set of privileges assigned to each role support the RBAC SFP.
- (b) The following critical information for performance of RBAC Administration functions is made available by the TOE.

- (i) View the type of access on each object by each user
- (ii) View the date and time of each access instance
- (iii) The Role that enabled that access

For fulfilling the above objectives, it is necessary to specify:

- (i) The Nature of information in the audit record (FAU\_GEN.1)
- (ii) The association between the audit event and the identity of the user (FAU\_GEN.2)
- (iii) The events that will trigger the generation of audit records (FAU\_SEL.1)
- (iv) Provision of capability to view, sort and search audit records to a restricted set of users (FAU\_SAR.1, FAU\_SAR.2 & FAU\_SAR.3)
- (v) Storage of Audit records in a permanent storage (FAU\_STG.1)

Depending upon the criticality of the data, it may be necessary to specify the following additional requirements in some software environments. However these are not considered core requirements for supporting access control through RBAC and hence not included in this PP. They may however need to be specified in the PP of the software for which access control function is implemented through RBAC mechanism. These are:

- (a) Produce automatic alerts in case of security violation (FAU\_ARP)
- (b) Analytical capability to detect various kinds of anomalies (FAU\_SAA)
- (c) Measures for guaranteeing the availability of audit logs (FAU\_STG.2) as well as actions required for recovering from (FAU\_STG.3) and prevention of (FAU\_STG.4) audit data loss.

### **B.3.2 Rationale for User Data Protection (FDP) Class Components**

The objectives behind the choice of User Data Protection components are:

- (a) Specify the scope of the RBAC SFP in terms of subjects, objects and operations that are covered
- (b) Specify RBAC relevant user, subject and object security attributes that are responsible for authorizing or denying access for users/subjects to objects.

The component FDP\_ACC.1 meets objective (a) while component FDP\_ACF.1 meets objective (b).

A more detailed explanation of the rationale behind the choice of the above components is as follows: In many software environments where RBAC is implemented it may be restrictive to stipulate that the entire set of objects under the control of the TOE be covered under RBAC SFP. We should therefore allow for the possibility of other access control SFPs to coexist with RBAC SFP for the same TOE. Hence, the component FDP\_ACC.1, which stipulates Subset Access Control, has been chosen.

The component FDP\_ACF.1 is used to express the core concept behind RBAC (i.e. that all *types of accesses* (operations) on the objects covered by RBAC SFP should be mediated by the

Role). Hence all access authorizations (access denials) should take place based upon the fact that the user is assigned (or not assigned) to that role whose privilege set includes (or not includes) that particular operation on the object.

The reasons for exclusion of certain families of requirements under the category of User Data Protection from RBAC PP are given below:

RBAC is essentially a model for access control based on the abstraction of roles and hence does not address information flow issues. Hence, the components FDP\_IFC and FDP\_IFF have not been included.

RBAC is concerned with restrictions on the type of access to data objects but not on the validity or authenticity of their information content. Hence, the family FDP\_DAU is not used.

This PP does not also cover requirements under FDP\_ETC and FDP\_ITC that govern export and import of data to & from outside TSF control. The export and import functions in most TOE implementations are handled by separate utilities. It is not necessary that those functions be covered under RBAC SFP since those functions deal with data at a much coarser level of granularity (e.g. bulk data transfers) than the objects whose access are typically covered by a RBAC SFP.

Since RBAC PP does not cover the requirements for distributed systems FDP\_ITT family has not been included. RBAC PP may cover access control requirements for various categories of applications. The allocation and deallocation of resources have different semantics between different systems. For example, allocation of a secondary storage device in an operating system may refer to a Disk Volume Unit but may refer to a named virtual disk segment in the case of a DBMS. Hence FDP\_RIP (residual information protection) cannot be specified as a requirement for an access control mechanism like RBAC but should be specified in the PP of the software for which RBAC SFP has been enforced. The same argument applies to the component FDP\_ROL (Rollback) as well. In this case, it is the nature of the TOE and the type of data under its control that determines the operations that can be rolled back and their associated objects and boundary conditions.

The kind of integrity errors and the kind of data attributes that are used for monitoring very much depend upon the kind of user data. For files, the attributes may involve UFIDs (Unique File Identifiers), File Allocation tables, and directory tree pointers. For database data, the attributes may be references to physical O/S files and pointers in the database object allocation tables. Hence it is not practical for a RBAC PP, which deals with a higher level access control mechanism, to specify integrity errors and data attributes for ensuring stored data integrity, since the requirements will be dictated by the nature of data. Hence, FDP\_SDI family is not considered.

Again the fact that RBAC is a higher level access control mechanism precludes the need to specify the confidentiality (FDP\_UCT) and preservation of integrity (FDP\_UIT) of the user data when it is transferred between the TOE and another trusted IT product.

### **B.3.3 Rationale for Identification and Authentication (FIA) Class Components**

Since RBAC is mainly an access control mechanism, Identification and Authentication requirements for a product or a class of product that supports RBAC, pertain only to the extent to which they support the access control requirements (Class FDP) and Security Management (Class FMT) requirements. The objectives that are sought to be fulfilled through the choice of Identification and Authentication components are:

- (a) Ability to associate the necessary set of attributes required for supporting RBAC with the user identity.
- (b) Authenticate the user before invoking any TSF that has been implemented to enforce RBAC SFP.
- (c) Identify the user before invoking any TSF that has been implemented to enforce RBAC SFP.
- (d) Ability to associate user security attributes (e.g. Assigned Role) to a subject acting on behalf of a user (e.g. an executable, a DBMS Stored Procedure) through the mechanism of roles.

The components FIA\_ATD.1, FIA\_UAU.2, FIA\_UID.2, and FIA\_USB.1 have been chosen to meet the objectives (a), (b), (c) and (d) respectively.

The nature of the authentication mechanism is not the concern of RBAC although it needs to be specified in the PP of the software product for which RBAC is to be implemented. Hence, the components FIA\_UAU.3, FIA\_UAU.4, FIA\_UAU.5, FIA\_UAU.6, and FIA\_UAU.7 have all been left out of consideration. Similar arguments apply to the requirements for specifying a set of actions to handle authentication failures and hence the component FIA\_AFL.1 is not included as well. Further the mechanics of generation of secrets is outside the scope of RBAC requirements and hence the requirements FAU\_SOS.1 and FAU\_SOS.2 have also been not specified.

### **B.3.4 Rationale for Security Management (FMT) Class Components**

The security management deals with the management of security attributes, TSF data, and functions. While the actual TSF functions required supporting RBAC may be implementation dependent, we can identify the security attributes and the broad categories of TSF data in this environment. These are given in the following table:

TSF relevant information category	Name of the entity
User Security Attribute	User Role Authorizations
User Security Attribute	User Default Active Role set
Object Security Attribute	Roles which can invoke the various operations
TSF Data	Role definitions & Role Attributes
TSF Data	Relationships among roles
TSF Data	Constraints among Role Relationships

Our objective in choosing components from the Security Management class is therefore as follows:

.

- (a) Restrict the right to modify the user security attributes to a set of RBAC administrators and object security attributes to (i) a set of RBAC administrators and (ii) Object Owners.
- (b) Specify constraints on the individual values of the attributes as well among the relative values among several attributes such that they can be automatically enforced at the time of data entry/ modification of the security attributes.
- (c) Provide the facility to generate default values for object security attributes
- (d) Restrict the right to create, modify TSF data to a set of RBAC administrators
- (e) Specify constraints on the individual values of the TSF data as well among the relative values among several TSF data items such that they can be automatically enforced at the time of data entry/ modification of TSF data
- (f) Restrict the right to revoke security attributes to a set of RBAC administrators and specify the conditions under which revocation will take place.
- (g) Specify the set of roles that should be authorized to perform all security relevant functions.

In order to meet the above objectives the components FMT\_MSA.1, FMT\_MSA.2, FPT\_MSA.3, FMT\_MTD.1, FMT\_MTD.3, FMT\_REV.1, and FMT\_SMR.2 have been included in the PP.

The following are the reasons for non-inclusion of other components and families from the Security Management class:

- (a) In the RBAC context, the limits for various data items in the TSF data (which consists of role definitions, role relationships, and constraints on role relationships) are to be specified as constraints and automatically enforced during data entry/modification. Since we have already specified through FMT\_MTD.3 that only secure values are to be accepted for TSF data, there is no need to specify the component FMT\_MTD.2 which provides the requirements for the RBAC administrator to be able to specify limits on TSF data and the actions to be performed in the event of limits getting exceeded.
- (b) For effective implementation of RBAC, all that is required is that there should be a designated RBAC administrator role which should be assigned to a limited set of users so as to perform all management functions with respect to RBAC SFP enforcing TSF functions, TSF data and security attributes. Depending upon the size and complexity of the software environment, there could be multiple administrative roles and in that context, conditions for assignment and activation of different roles must be satisfied. The overall administrative model therefore is implementation dependent and hence the components FMT\_SMR.2 and FMT\_SMR.3 have not been included in the RBAC PP.

### **B.3.5 Rationale for Protection of TOE Security Functions (FPT) Class Components**

In order to ensure that TSFs effectively implement the RBAC SFP, we require that:

- (a) the platform on which the TSF has been implemented has to be proven to meet certain security

assumptions.

- (b) we have a suite of tests to verify the correct operation of TSF as well as verify the integrity of TSF data and executables
- (c) we can specify the list of failures under which TSF will preserve a secure state
- (d) TSF provides the RBAC administrator with the capability to restore the TSF Data (RBAC database) to a consistent and secure state after a failure.
- (e) we can specify the failure scenarios that have the atomicity property (i.e. the security function either completes successfully or recovers to a consistent and secure state)
- (f) RBAC SFP enforcing TSFs cannot be bypassed ( a counter example is accessing a database through a COTS product instead of a home grown application)
- (g) RBAC SFP enforcing TSFs operate in their own security domain and cannot be invoked or manipulated from other domains

In order to meet the above objectives the components FPT\_AMT.1, FPT\_TST.1, FPT\_FLS.1, FPT\_RCV.1, FPT\_RCV.4, FPT\_RVM.1, and FPT\_SEP.1 have been included.

FPT\_STM.1 is included because FAU\_GEN.1 depends on it.

The following are the reasons for the non-inclusion of other families of requirements from this FPT class. They should be considered for inclusion in the software product PP for which RBAC has been implemented depending upon its architecture. They are:

- (a) When a software product for which RBAC has been implemented exchanges data with a remote trusted IT product, the availability requirements (specified through family FPT\_ITA), confidentiality (FPT\_ITC), integrity (FPT\_ITI) and consistency (FPT\_TDC) are critical security requirements for the overall product and hence should be included in the software product PP. In this RBAC PP we are only concerned with the protection of TSFs that enforce RBAC SFP and not with the overall security of the communication channel that enables secure communication of TSF data with an outside trusted IT product. A typical example for this type of scenario is an enterprise administration tool that maintains RBAC administrative data but the TSFs that actually enforce access control are part of the various isolated application systems. In this case, what is required is the secure transfer of RBAC administrative data from the administration tool to the individual systems to enable native access control TSFs in those systems to enforce the RBAC SFP.
- (b) A similar argument as above holds good when RBAC SFP enforcing TSFs have been implemented as distributed software. Hence, FPT\_ITT (internal TOE data transfer) and FPT\_TRC (internal TOE data replication consistency) have not been included as well.
- (c) The overall physical protection for TSF (FPT\_PHP) should be included under the overall Organizational Security Policy and hence there is no need for it to be included in the RBAC PP.

### **B.3.6 Rationale for TOE Access (FTA) Class Components**

The main motivation behind the RBAC SFP is that all the access rights on data objects under

the control of the TOE that the user has must be acquired through the roles that have been authorized for the user. A subset of this set of authorized roles is the Active Role Set (ARS), which is that set of roles that have actually been activated for the user in a particular session. This ARS, therefore, determines the total privilege set for the user in a session and hence is a session security attribute. In many software environments, the user should have the flexibility to add or delete members (i.e. change the composition) of this ARS. However, the scope of this choice should be limited to the set of roles authorized for the user by the RBAC Administrator.

Further in order for the user to have an initial set of access rights at the start of the session, the RBAC administrator has to specify a default active role set (DARS) whose composition can then be altered by the user during the course of the session.

Based on the above discussion, the objectives behind the choice of components from the TOE Access (FTA) are:

- (a) ARS being a session security attribute, the scope of changes on this should be limited to the set of authorized roles for the user.
- (b) The Default Active Role Set (DARS) which determines the initial access rights for a user in a session should be a non-empty or non-null set. If it happens to be a null set, the session manager should prevent the user from establishing the session.

The selected components FTA\_LSA.1 and FTA\_TSE.1 meet the above objectives by using ARS & DARS.

Apart from mediating access in a TOE session through the mechanism of active role set (ARS), it is outside the scope of RBAC PP to stipulate the requirements that pertain to the management of the various parameters associated with a session. Hence, the following families of requirements have been left out of consideration. They are:

- (a) Ability to limit the number of concurrent sessions (FTA\_MCS)
- (b) Ability to specify events that can lock or unlock an active session (FTA\_SSL)
- (c) Advisory warnings re: inappropriate use of TOE (FTA\_TAB)
- (d) Display access history information (FTA\_TAH).

#### **B.4 Satisfaction of IT security objectives**

The following table B.1 portrays the relationship of the functional requirement components to the RBAC IT security objectives they are intended to satisfy.

Every IT security objective is shown to be met by at least one functional requirement component. The analysis previously given in section B.3 demonstrated the reverse argument, that every functional requirement is supportive of at least one IT security objective.



**Table B.2 - Mapping objectives to functional requirements**

<b>Security Objective</b>	<b>Functional Requirement Components</b>
<b>O.ACCOUNT</b> The TOE must ensure that all users can be held accountable for their security relevant actions.	FAU_GEN.1-2, FAU_SAR.1-3, FAU_SEL.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FPT_STM.1
<b>O.ADMIN</b> The TOE must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.	FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FIA_UAU.2, FIA_UID.2, FMT_MSA.1-2, FMT_MTD.1&3, FMT_REV.1, FMT_SMR.2, FPT_AMT.1, FPT_FLS.1, FPT_RCV.1, FPT_RCV.4, FPT_TST.1
<b>O.AUDIT</b> The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.	FAU_GEN.1-2, FAU_SAR.1-3, FAU_SEL.1, FAU_STG.1, FPT_STM.1
<b>O.DUTY</b> The TOE must provide the capability of enforcing 'separation of duties', so that no single user has to be granted the right to perform all operations on important information.	FDP_ACC.1, FDP_ACF.1, FPT_SEP.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_SMR.2, FPT_RVM.1, FTA_LSA.1
<b>O.ENTRY</b> The TOE must strongly prevent logical entry to it by persons or processes with no rights to access it.	FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1
<b>O.HIERARCHICAL</b> The TOE must allow hierarchical definitions of roles. Hierarchical definition of roles means the ability to define roles in terms of other roles. This saves time and allows more convenient administration of the TOE.	FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MTD.1, FMT_SMR.2, FPT_RVM.1, FPT_SEP.1, FTA_LSA.1
<b>O.KNOWN</b> Legitimate users of the system must be identified before rights of access can be granted.	FIA_ATD.1, FIA_UID.2, FIA_USB.1, FMT_MSA.1
<b>O.ROLE</b> The TOE must prevent users from gaining access to and performing operations on its resources/objects unless they have been granted access by the resource/object owner or they have been assigned to a role (by an authorized administrator) which permits those operations.	FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MSA.3, FPT_RVM.1, FPT_SEP.1, FTA_LSA.1, FTA_TSE.1

## B.5 RBAC Functional requirements dependencies

Functional components possess dependencies, which are stated requirements for the RBAC PP to include further components in support of the primary requirements.

To meet the evaluation requirements, it is necessary for all dependencies to be satisfied. Table B.3 below demonstrates how the dependencies of each included component have been satisfied.

All of the components of the RBAC PP are listed with a numeric line number. The dependencies of each component, if any, are listed alongside that component with a reference to the line number of the component that satisfies them. In the case of assurance component dependencies, all are satisfied hierarchically by assurance level EAL3, which is given as the reference. Component reference line numbers followed by '(H)' indicate that the dependency is satisfied by a hierarchical component to that referenced.

This table demonstrates that RBAC has no unsatisfied dependencies.

**Table B.3 - RBAC functional component dependency analysis**

Line Number	Component	Dependencies	Reference Line
1	FAU_GEN.1	FPT_STM.1	27
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 12(H)
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	1 17
7	FAU_STG.1	FAU_GEN.1	1
8	FDP_ACC.1	FDP_ACF.1	9
9	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	8 18
10	FIA_ATD.1		
11	FIA_UAU.2	FIA_UID.1	12(H)
12	FIA_UID.2		
13	FIA_USB.1	FIA_ATD.1	10
14	FMT_MSA.1	FDP_ACC.1 FMT_SMR.2	8 20
15	FMT_MSA.2	FDP_ACC.1 FMT_MSA.1	8 14

		FMT_SMR.2 ADV_SPM.1	20
16	FMT_MSA.3	ADV_SPM.1 FMT_MSA.1 FMT_SMR.2	14 20
17	FMT_MTD.1	FMT_SMR.2	20
18	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	17
19	FMT_REV.1	FMT_SMR.2	20
20	FMT_SMR.2	FIA_UID.1	12(H)
21	FPT_AMT.1		
22	FPT_FLS.1	ADV_SPM.1	
23	FPT_RCV.1	FMT_SMR.2 FPT_TST.1 ADV_SPM.1 AGD_ADM.1	20 28
24	FPT_RCV.4	ADV_SPM.1	
25	FPT_RVM.1		
26	FPT_SEP.1		
27	FPT_STM.1		
28	FPT_TST.1	FPT_AMT.1	21
29	FTA_LSA.1		
30	FTA_TSE.1		

## B.6 Strength of Function Rationale

SOF-basic is commensurate with an assurance requirement of EAL2.

## B.7 RBAC Assurance requirements rationale

The assurance requirements for RBAC are portrayed in Table B.4 below. The rationale for the assurance requirements is stated following the table.

**Table B.4 - RBAC assurance requirements**

Requirement	Name
EAL2	Structurally Tested

ADV_SPM.1	Informal TOE Security Policy Model
-----------	------------------------------------

### **B.7.1 Evaluation assurance level rationale**

#### **EAL2- Structurally Tested**

Role-Based Access control is intended to be used in a wide range of software applications such as commercial DBMSs, Firewalls, encryption devices, etc. Products that implement Role-Based Access Control have widely varying security requirements. This PP requires minimal assurance that RBAC-relevant functions are implemented correctly. For COTS products, it will be difficult to obtain evidence of tests that provides complete coverage of all functional specifications and high-level design features, as required by a higher EAL. Hence, EAL2 has been chosen as the minimum EAL for the RBAC PP.

### **B.7.2 Assurance augmentations rationale**

#### **ADV\_SPM.1 Informal TOE Security Policy Model**

This assurance component is required as a dependency for these functional components: FMT\_MSA.2, FMT\_MSA.3, FMT\_MTD.3, FPT\_FLS.1, FPT\_RCV.1, and FPT\_RCV.4.